Brainae Journal of Business, Sciences and Technology
ISSN "2789-374X (print)" "2789-3758 (online)
Volume 26, Issue 6, June 2023
http://www. brainajournal.com info@brainae.org

L'ENJEU DES DONNÉES À CARACTÈRE PERSONNEL DANS LE PROCESSUS BIOMÉTRIQUE : LA DIGNITÉ HUMAINE EST-ELLE RESPECTÉE ?

Par

Dr. Christ Hermann POUNAH

Doctorat en Droit, Maître Assistant

Mobile +241 77474400

E-mail : hermannchrist@gmail.com

Reçu : 09 Mai, 2023 ; **Accepté** : 29 Mai, 2023 ; **Publié :** 06 Juin 2023

Résumé :

Aujourd'hui sur le continent africain, la biométrie tend à transformer la vie des populations eu égard aux innombrables exemples à travers lesquels elle révolutionne les technologies pour améliorer leurs pratiques : le *mobil-banking*, la connexion des téléphones portables qui plus que jamais fait fi des lignes de téléphone fixe.

Désormais, le continent noir a adopté la technologie de la biométrie. Mesurant les particularités physiques propres à chaque personne, généralement par la reconnaissance des empreintes digitales, du visage ou de l'iris, les solutions biométriques peuvent aisément authentifier l'identité.

Néanmoins, au sein de certains écosystèmes biométriques, la protection des données inquiète, surtout lorsqu'il s'agit de données personnelles dites sensibles. Pourtant, il convient de comprendre qu'une protection adéquate de la vie privée des citoyens ainsi que la sécurisation des données qui leur sont prélevées est un double défi qui doit être relevé, tant pour l'adoption généralisée de la biométrie en Afrique, que pour son exploitation pour le plus grand bénéfice de nos sociétés.

Mots clé : *données à caractère personnel, biométrie, dignité humaine.*

Abstract:

Today on the African continent, biometrics tends to transform people's lives with regard to the countless examples through which it is revolutionizing technologies to improve their practices: mobile banking, the connection of mobile phones which more than ever ignores landline telephone lines.

Now, the black continent has adopted the technology of biometrics. Measuring the physical particularities specific to each person, generally by the recognition of the fingerprints, the face or the iris, the biometric solutions can easily authenticate the identity.

Nevertheless, within certain biometric ecosystems, data protection is a concern, especially when it comes to so-called sensitive personal data. However, it should be understood that adequate protection of the privacy of citizens as well as securing the data collected from them is a double challenge that must be met, both for the widespread adoption of biometrics in Africa, and for its exploitation for the greater benefit of our societies. ***Keywords***: *personal data, biometrics, human dignity.*

Introduction :

Les données à caractère personnelles (DP) sont des informations qui permettent d'identifier directement ou indirectement une personne physique. Elles sont protégées par divers instruments juridiques[1] concernant le droit à la vie privée. À l'instar de la CNIL française et de la Commission Nationale pour la Protection des Données Personnelles (CNPDCP) au Gabon, nombre de pays disposent aujourd'hui d'autorités chargées de la protection des données personnelles, qui sont souvent des autorités administratives indépendantes (ou des équivalents de celles-ci).

Les DP (ou données nominatives) correspondent notamment aux noms, prénoms, adresses (physique et électronique), numéro de téléphone, lieu et date de naissance, numéro de sécurité sociale, numéro de carte de paiement, plaque d'immatriculation d'un véhicule, photo, empreinte digitale, ADN.

Aujourd'hui, en effet, une prospection à l'aide d'un moteur de recherche sur une ou plusieurs bases de données, en utilisant simplement la combinaison de quelques-uns de ces éléments permet d'identifier et de retrouver avec une précision étonnante n'importe quel individu dument répertorié. Certaines de ces données, dont en particulier le numéro de sécurité sociale ou le NIR[2], ainsi que les données biométriques (empreinte digitale, échantillon ADN[3]), sont particulièrement sensibles, car elles fonctionnent en tant qu'« identifiants universels ».

« *Nous définirons la biométrie comme une technique d'identification et d'authentification qui consiste à transformer les caractéristiques biologiques, génétiques et comportementales d'une personne telles que les empreintes digitales, l'empreinte de l'iris, de la rétine, de la voix, de la forme du visage, de la forme de la main, en une empreinte numérique. Venant du grec « bios » (vie) et de « metron » (mesure), cette technique permet de mesurer le vivant à partir des parties du corps considérées comme inchangeables. Avec elle, l'identité est réduite aux caractéristiques physiques et génétiques qui attestent de l'unicité d'une personne.* ». (Ceyhan, 2006).

Il est dès lors aisé de se rendre compte que plusieurs éléments essentiels sont pris en compte concernant ce type de données, dont leur durée de conservation, leur finalité, le consentement de la personne vis-à-vis de cette collecte des données personnelles, l'obligation d'information et, dans le cadre de l'entreprise, la consultation des instances représentatives, le niveau de protection technique dont elles bénéficient ou non.

1- Constat

Malheureusement et indépendamment de toutes les garanties qui semble-t-il, entourent la collecte de ce genre d'information, le « risque zéro » n'existe pas.

Les modes de collecte se sont particulièrement diversifiés avec les technologies numériques : du formulaire rempli volontairement par les individus à l'enregistrement de traces (habitude de navigation, localisation géographique de l'adresse de connexion).

Les modes d'exploitation peuvent être le fait des individus eux-mêmes par la recherche d'informations à partir d'un moteur de recherche, sur les réseaux sociaux en ligne ou via certaines organisations (marketing ciblé, fichage des populations par l'État, envoi massif de courriers non sollicités à caractère commercial). Se pose donc la question de savoir ce qui pourrait advenir en cas d'usage fallacieux de ces données d'où, la pertinence de la thématique du **« respect de la dignité humaine dans la collecte des données à caractère personnel »**.

La « thétique » sus-évoquée, trouve son intérêt dans le contexte actuel du fait que l'on observe une inquiétude de la part des populations et même des sociétés civiles des Etats au sein desquels sont mis en place les différents systèmes de collecte des données tantôt mentionnés, en l'occurrence lorsqu'il s'agit d'échéances électorales.

« *Le premier recensement biométrique au Somaliland, à l'occasion de l'élection présidentielle de 2010, est un cas paradigmatique d'une technologie adoptée à la hâte qui débouche sur un recensement (soutenu financièrement par des bailleurs qui donnèrent plus de 10 millions de dollars) désastreux*[4]*.*
C'est une entreprise européenne, Copenhagen Elections, qui remporte le marché. Elle sous-traite les opérations à une entreprise indienne, Electronics Company of India. Or, celle-ci n'est pas spécialisée dans les élections et se heurte à de sérieux problèmes logistiques et techniques[5]*.*

Tout est fait dans l'urgence : le matériel n'a pas été suffisamment testé, le software n'est pas prêt au lancement des opérations de recensement, la formation des agents recenseurs est incomplète [...] Rien ne se passe comme prévu pour cette grande opération visant à doter le Somaliland d'une liste électorale fiable.

[1] En France il s'agit notamment de la loi Informatique, fichiers et libertés de 1978, la directive 95/46/CE au niveau communautaire ainsi que la Convention n°108 pour la protection des données personnelles du Conseil de l'Europe. Au Gabon il y a la Loi n° 1/2011 du 25 septembre 2011 relative à la protection des données à caractère personnel.

[2] Numéro d'Inscription au Répertoire National d'Indentification des Personnes Physiques.

[3] Selon une déclaration du Conseil des ministres du Conseil de l'Europe de 1997, elles incluent les données médicales et génétiques, ainsi que les empreintes digitales et, en général, toute caractéristique biométrique.

[4] Somaliland: A Way out of the Electoral Crisis, International Crisis Group, 2009, p. 6

[5] Anna C. Rader, Verification and Legibility in Somaliland's identity architecture, Department of Politics and International Studies, University of London, 2016

Au final, les données collectées sont de trop mauvaise qualité pour être exploitées : plus de la moitié des personnes enregistrées dans la base l'ont été sans empreintes. Dans un contexte politique déjà tendu, ces difficultés viennent jeter de l'huile sur le feu : le parti présidentiel et l'opposition se déchirent, le conflit s'étend à la rue où des affrontements avec la police font plusieurs morts. Le Somaliland ne fait cependant pas marche arrière : le pays s'engage au contraire dans une surenchère technologique en adoptant pour l'élection présidentielle suivante, en 2017, le scanning de l'iris des yeux [...]. ». (Debos, 2021).

Ainsi, les sujets intéressés s'interrogent t-ils parfois sur l'usage réel qui en sera fait, lorsqu'ils ne voient pas carrément, une atteinte à leurs droits les plus fondamentaux. De multiples exemples révèlent, si besoin est, la perplexité et la subtilité que revêt le maniement des données à caractère personnel.

La Conférence Internationale sur la protection des données personnelles avait mis sur pied, en 1983, un groupe de travail spécifique qui visait à protéger les données à caractère personnel dans le domaine des télécommunications, le célèbre « International Working Group on Data Protection in Telecommunications » (IWGDPT).

Quelle ne fût pas la surprise lorsque quelques années plus tard, le grand public apprenait l'existence du réseau ECHELON[6] et la redoutable puissance du renseignement d'origine électromagnétique moderne.

C'est d'ailleurs pour cette raison que la CNIL en France, et son homologue européen le G29[7], considèrent que l'échange de ces données entre États ainsi que l'utilisation qui en est faite soulèvent un certain nombre de problèmes quant au respect de la vie privée, particulièrement avec les États-Unis dont la législation protège moins bien ces données que ne le fait la législation de l'Union Européenne (UE). L'on s'aperçoit nettement des réactions que suscite cette collecte même au sein des pays occidentaux, qui pourtant demeurent largement en avance sur certains aspects par rapport à ceux du continent africain.

2- De la nécessité d'encadrer la collecte des DP

Dans son œuvre Les Pensées, Blaise PASCAL relevait le fait que : « *Le droit sans dignité n'est que médiocrité et la dignité sans droit n'est que déraison* » cette assertion nous amène à penser à un encadrement sans doute pas parfait, mais néanmoins adéquat de la collecte des DP car au XXI[ème] siècle, les nouvelles technologies sont devenues plus que jamais des notions clefs de nos sociétés contemporaines, s'immisçant dans tous les domaines du réel, notamment dans le domaine de la protection des droits humains ; elles finissent par toucher aux questions relatives à la bioéthique, au progrès médical, aux dispositifs d'espionnage et de vidéosurveillance, à la collecte de différents types de données, à l'identification et à la localisation des personnes.

A priori, on peut considérer que ces avancées ne peuvent que favoriser les droits de chacun tout en nous en enrichissant. Toutefois, qu'en est-il du progrès dès lors qu'il devient une source de danger pour les droits humains, notamment lorsque son incidence n'a pas fait l'objet d'une réflexion ou parfois même d'aucun encadrement juridique, éthique voire même sociologique ?

« *En ce qui a trait aux failles (ou aux inconvénients) des technologies biométriques, les arguments soulevés par les opposants concernent davantage les systèmes d'information et sont liés :*

- *aux menaces de la collecte non nécessaire ;*
- *au traitement (risque de restreindre les libertés individuelles) ;*
- *à la communication (non autorisée) des informations ;*
- *à l'interconnexion des bases de données facilitée par le recours à un identifiant unique (finalité) ; et*
- *au coût.*

Par rapport aux caractéristiques de la biométrie, les principaux arguments des opposants sont les suivants :

- *information intrinsèquement liée à la personne (possibilité de découvrir des maladies) ;*
- *nécessité de se soumettre physiquement au processus de vérification (méthode considérée intrusive) ;*
- *difficulté de se défaire de ses caractéristiques biométriques (unicité de la donnée) et difficulté d'apporter la preuve que la personne n'a pas commis les actes qui lui sont imputés en cas de falsification (faux élément biométrique) ou d'usurpation (vol du fichier de signature) d'identité ;*

- *Comparaison biométrique qui apporte un taux d'incertitude sur la validité du client accepté (fausse acceptation) ou refusé (faux rejet), au contraire de l'utilisation des systèmes traditionnels d'authentification, tel le mot de passe ou le jeton, qui produisent une réponse sûre à 100 % (vrai ou faux). ».*

[6] Le « réseau Echelon de surveillance et d'interception globale des télécommunications à l'échelle mondiale » a été initialement mis en place par les Etats-Unis pour des raisons de sécurité militaire. Au même titre que le Canada, la Nouvelle-Zélande et l'Australie, le Royaume-Uni participe effectivement à ce dispositif.

[7] Le G29, ou groupe de l'article 29, est un ancien organe de l'Union européenne. Il regroupe plusieurs membres représentant l'autorité des différents pays européens. Le rôle de cette instance est de vérifier la bonne application et la cohérence des règles sur la protection des données dans les différents pays européens.

Les différents arguments supra relevés induisent dans une certaine mesure, la nécessité d'établir des règles visant à faire respecter la vie privée de chaque individu et cela n'est possible que par une consécration des principes inaliénables que sont le respect des libertés individuelles des personnes physiques et de la vie privée. Retenons toutefois, que la notion de « vie privée » est une notion large non susceptible d'être définie de manière exhaustive. En effet, la vie privée englobe de multiples aspects de l'identité physique et sociale des individus.

Il s'agit du droit pour chaque personne, quels que soient ses rangs, sa naissance, sa fortune, son âge, de voir respecter sa vie privée et intime. En France, ce principe est affirmé par l'article 9 du Code civil et revêt même une « valeur constitutionnelle ».

Les éléments constitutifs de la vie privée sont notamment la santé, la vie sentimentale et familiale, la religion, le domicile, les revenus, les convictions politiques. C'est donc la situation à caractère privé ou public et le lieu de situation (vie personnelle, vie sociale) qui donnent le droit à chacun de s'opposer à la publication d'informations personnelles.

En ce quasi début de troisième millénaire, le problème a pris une nouvelle importance compte tenu de l'immixtion des technologies de l'information et de communication (TIC) dans nos vies. Plus que jamais la question de la conciliation entre TIC et vie privée se pose avec acuité[8]. Les diverses perspectives ouvertes par la généralisation et le perfectionnement des techniques informatiques deviennent de plus en plus dangereuses.

Le fichage de données par exemple tend à faire naître une sorte de psychose chez les individus, car ne sachant pas ce qu'il sera fait des informations confidentielles à caractère personnel enregistrées électroniquement. Il n'est pas non plus sans intérêt de souligner le fait que l'usage croissant du traitement automatisé des données à caractère personnel accroit inexorablement le risque d'utilisation illicite ou illégale desdites données. Lorsqu'il s'agit d'aborder la question de la menace des nouvelles technologies pour les droits humains, les atteintes demeurent légions.

3- Données personnelles et biométrie

La question reste posée quant à la menace des DP dès lors qu'il s'agit de la biométrie. En effet, les atteintes aux libertés individuelles des personnes physiques peuvent se faire par le truchement des données biométriques[9]. Ces données sont des caractéristiques biologiques numérisées et spécifiques à chaque être humain. Elles sont donc « identifiantes » et recueillies en présence de l'individu (et peuvent aussi bien servir à des fins administratives et/ou sécuritaires) ou à son insu via les caméras de surveillance, les empreintes digitales, l'ADN et même d'enregistrement vocal.
Aussi, les pouvoirs publics peuvent s'immiscer dans notre vie privée dès lors :

- Que la sécurité nationale ou publique ou le bien-être économique du pays sont mis en péril ;
- Qu'il s'agit de prévenir des désordres ou des faits délictueux ;
- Qu'il faut protéger la santé, les bonnes mœurs ou les droits et libertés.

Il faut relever que les données à caractère personnel sont des données sensibles et fragiles, car souvent mal protégées. Elles ont de la valeur et sont donc objets de convoitises. Ce phénomène ne connaît aucune limite et touche tous les domaines d'activités. Subséquement, l'utilisation croissante du traitement automatisé des données à caractère personnel ces dernières années n'a fait qu'accroître le risque d'utilisation illicite ou illégale des données à caractère personnel, tout en facilitant leur transfert par-delà les frontières entre pays avec des niveaux de protection très différents pour ces données.

Face à la nécessité de concilier certains droits fondamentaux et de garantir le même niveau de protection pour ces droits au-delà des frontières propres à chaque Etat, les gouvernements s'organisent afin de garantir la protection d'un droit fondamental, intrinsèquement lié à l'être humain.

Heureusement pour le citoyen, lorsqu'il est question de collecter des données personnelles dans le cadre de la conception des fichiers biométriques, les Etats prennent le soin de préciser que ces dernières seront collectées et traités de manière loyale et licite et ce, pour des finalités déterminées, explicites et légitimes. Il pèse donc sur le collecteur et même sur celui qui procèdera au traitement, une obligation légale.

4- Des mécanismes de protection

Pour parer toute éventualité, la Loi n° 1/2011 du 25 septembre 2011 relative à la protection des données à caractère personnel prise en application des dispositions des articles 1er et 47 de la Constitution

[8] Il y a très souvent au sein de certains Etats, des problèmes de criminalité tels l'usurpation ou le vol d'identité. Ce type de criminalité peut constituer un problème individuel (un citoyen, victime d'une usurpation d'identité) mais aussi, à plus large échelle, un problème qui touche la collectivité lorsqu'il y a usage abusif des services gouvernementaux offerts à la population à partir des contributions de l'ensemble des citoyens. Eu égard à ce dernier cas, il est tout à fait légitime de se demander quelles mesures un gouvernement peut utiliser pour s'assurer de réserver l'admissibilité à ses services aux ayants droit.

[9] L'usage de la biométrie engendre nombre d'interrogations notamment en ce qui concerne le respect des droits humains, ainsi que la législation sur le traitement automatisé des données à caractère personnel. En effet, à l'instar de toute nouvelle technologie, de nombreux doutes sont émis quant à la maturité, la fiabilité des techniques ainsi que sur la capacité à garder le contrôle de systèmes biométriques déployés à grande échelle.

Il s'agit pour certains, d'une nécessaire application du principe de précaution afin de faire face au développement irréversible et imprévisible de la biométrie dans le monde. Pour d'autres, il est à craindre que la biométrie ne devienne *in fine*, un instrument de contrôle et de surveillance trop puissant entre les mains de la puissance publique.

gabonaise, a pour objet de mettre en place un dispositif permettant de lutter contre les atteintes à la vie privée qui pourraient survenir lors de la collecte, le traitement, la transmission, le stockage et l'usage des données à caractère personnel. En effet, et c'est tout à son honneur que le législateur gabonais part du principe selon lequel, les TIC se doivent d'être au service de chaque citoyen. Pour cette raison, leur développement doit donc s'opérer dans un cadre strictement règlementé, sans qu'aucune atteinte ne soit portée ni aux droits humains, ni à la vie privée, ni aux libertés individuelles ou publiques.

Au regard de la potentielle dangerosité de tels moyens, les mécanismes de protection quant au respect des individus doivent impérativement s'organiser par le truchement de divers moyens à l'instar :

- du devoir d'information des personnes concernées, quant à leurs droits et des responsables de traitements quant à leurs obligations ;
- de la vérification du traitement des données à caractère personnel (la confirmation que les données à caractère personnel d'une tierce personne feront ou ne feront pas l'objet d'un quelconque traitement autre que celui pour lequel il a été prévu), de leur surveillance du point de vue de leur mise en œuvre (informations relatives aux finalités du traitement)[10].

Relevons que le droit à l'anonymat[11] gagnerait à être pris en compte par le législateur gabonais (en France, l'anonymat est une liberté fondamentale et un droit de la personne protégée[12]). L'anonymat est très largement reconnu aujourd'hui, notamment en droit français : il s'agit d'un droit qui tien compte du respect de la vie privée et des libertés individuelles. Son contrôle est clairement encadré afin de ne pas laisser la porte ouverte à des actes d'incivismes et à des actions délictuelles. A cet effet, nul ne peut prétendre se cacher derrière son droit à l'anonymat pour violer les droits d'un tiers (atteinte à l'honneur d'autrui, non respect du droit à l'image, diffamation) ou enfreindre la loi.

[10] Nous déplorons simplement que sous nos cieux, cette exigence législative voire même règlementaire, n'est pas forcément prise en compte. En effet, lors de la collecte de vos données personnelles les agents collecteurs ne sont généralement pas diserts quant à l'usage qui sera fait des données prélevées.

[11] En France, le droit à l'anonymat est consacré par la Loi informatique et Liberté du 6/1/1978.

[12] Les établissements de santé (notamment les établissements publics) sont tenus de respecter le droit du patient à bénéficier d'une prise en charge anonyme. Les professionnels de santé doivent dès lors être informés de toute demande d'anonymat et mettre en œuvre des procédures adaptées, l'enjeu étant le maintien du lien de confiance entre la personne malade et l'établissement de santé (*cf.* Le droit au secret des informations : définition et fondement). D'un point de vue de la responsabilité juridique, le non-respect de ce droit peut entraîner de lourdes sanctions. https://www.weka.fr

L'obligation de garantir la sécurité des systèmes d'information constitue une pièce centrale des législations de protection des données à caractère personnel. Elle s'y conçoit dans un double sens : il s'agit autant d'assurer la confidentialité des données, c'est-à-dire le non accès à celles-ci par des personnes non autorisées, que leur fiabilité, c'est-à-dire la qualité des données traitées, leur exactitude, leur mise à jour et leur non déformation par le traitement. Certes, la protection des données ne se réduit pas à leur sécurité.

Elle repose également sur quatre principes :

- la participation individuelle, qui se conçoit à la fois comme la possibilité pour la personne concernée de connaître (l'accès) voire, dans certains cas, de maîtriser par le consentement ou l'opposition, la circulation de son image informationnelle ;
- la finalité, qui exige que les raisons pour lesquelles l'information nominative collectée soient déterminées, explicites et légitimes ;
- la proportionnalité, qui s'oppose à ce que le responsable du traitement traite plus de données que celles strictement nécessaires pour l'obtention des finalités ;
- la qualité des données, qui s'entend de l'exactitude et de la mise à jour des données.

A travers la Loi n° 1/2011 du 25 septembre 2011 relative à la protection des données à caractère personnel, le législateur gabonais ne se départit pas et à raison, de ce qui se fait partout ailleurs c'es-à-dire, établir un certain nombre de règles et de directives en mesure d'encadrer les technologies de l'information et de la communication eu égard à la collecte et au traitement des DCP.

L'article 3 de cette loi dispose d'ailleurs que « *Les technologies de l'information et de la communication doivent être au service de chaque citoyen. Leur développement doit s'opérer dans le cadre de la coopération internationale, dans la limite des accords en vigueur. Elles ne doivent porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques* ».

La coopération internationale peut être perçue ici, non pas comme certains le pensent à savoir, un mimétisme quant à ce qui se fait en occident, mais plutôt comme un moyen de profiter de ce qui se fait de mieux ailleurs au regard de l'expérience capitalisée et de l'avance considérable acquise dans le traitement de telles questions.

Pour ce qui est de la nécessité de ne point porter atteintes ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques, elle traduit naturellement la prise en application des articles 1 et 47 de la Constitution gabonaise, qui détermine les règles relatives au traitement des données à caractère personnel. De

façon décomplexée, l'objectif poursuivi est de lutter contre les atteintes à la vie privée susceptibles d'être engendrées par la collecte, le traitement, la transmission, le stockage et l'usage des DCP.

5- Suggestion

Une fois ce cadre bien précisé, il est à recommander que les commissions dans le cadre des pouvoirs d'enquête qui leur sont conférés prospectent sur la régularité des comportements et pratiques des différents acteurs situés tant sur le territoire national qu'à l'extérieur. A cet égard, ces entités répressives devraient disposer de moyens suffisamment étendus pour effectuer des vérifications de cette nature, voire constituer une entité spécifique pour la protection des utilisateurs. Par ailleurs il conviendrait par la même occasion, de relever le niveau général des sanctions afin d'être véritablement dissuasif face aux éventuels manquements des acteurs importants.

Conclusion

La notion de protection des « données à caractère personnel » est étroitement liée à celle de données concernant la vie privée. Pour les juristes, le texte fondateur de la vie privée, qui a directement orienté l'exercice de ces droits, est la Déclaration universelle des droits de l'homme et du citoyen. Si comme nous avons pu le voir, des règles de droit sont établies au niveau national et international, il semble que la difficulté se situe parfois au niveau de l'application et notamment de l'adaptation des mentalités à des activités relevant de l'immatériel et donc d'éléments n'ayant pas de corporalité.

Il semble dès lors nécessaire de réaliser une importante réflexion sur le travail pédagogique à mener, notamment en direction des citoyens afin qu'ils appréhendent au mieux des notions qu'il n'est pas toujours aisé d'apprécier.

A la question de savoir si la dignité humaine est respectée dans la collecte des données personnelles en République Gabonaise nous répondons par l'affirmative et précisons néanmoins, comme nous l'évoquions tantôt dans notre développement, que des améliorations substantielles doivent être faites afin que le processus de collecte de données personnelles et partant, le système biométrique ne demeure plus aussi compliqué à appréhender par le citoyen lambda (nombre de personnes s'accordant sur le fait que la biométrie n'est pas une panacée, mais est-ce vraiment son but ? Il s'agit ici d'un tout autre débat), mais qu'il soit de préférence fiable.

In fine, nous demeurons résolument convaincus que la valorisation de l'approche normative apparait comme un moyen efficace de répondre aux défis novateurs posés par la révolution des techniques de contrôle d'identité.

Références webographiques

Awenengo Dalberto, s. Banegas, r. et Cutolo, A. (2018). *Biomaîtriser les identités ? État documentaire et citoyenneté au tournant biométrique. Cairn.info, (4)152, 5-29.* Repéré à https://www.cairn.info/revue-politique-africaine-2018-4-page-5.htm

CEYHAN, A. (2006). *Enjeux d'identification et de surveillance à l'heure de la biométrie. Centre d'études sur les conflits lilberté et sécurité, L'Harmattan, 33-47.* Repéré à URL : http://journals.openedition.org/conflits/2176

Commission de l'éthique de la science et de la technologie. (2005). *L'utilisation des données biométriques à des fins de sécurité : questionnement sur les enjeux éthiques.* www.ethique.gouv.qc.ca

DAGNELIE, P. (1998). *Quelques perspectives relatives à la biométrie: pays en voie de développement et pays développés. Société française de Biométrie*, 15-28. Repéré à http://dagnelie.be/docpub/dagnelie-1998b.pdf

DEBOS, M. (2021). Biométrie électorale, un mirage démocratique. *Afrique XXI.* Repéré à https://afriquexxi.info/article4846.html

DUBEY, G. (2008). Nouvelles techniques d'identification, nouveaux pouvoirs. Le cas de la biométrie. *Presses Universitaires de France, « Cahiers internationaux de sociologie »* (2) 125, 263-279. Repéré à https://www.cairn.info/revue-cahiers-internationaux-de-sociologie-2008-2-page-263.

Groupe de la Banque Mondiale. (2014). *Guide de l'identité électronique à l'attention des parties prenantes d'Afrique*. Repéré à www.worldbank.org

Références bibliographiques

PASCAL, B. (2010). *Pensées, opuscules et lettres*. Paris : Classiques Garnier, 807 p.

CEYHAN, A et PIAZZA, P. (2014). *L'identification biométrique : champs, acteurs, enjeux et controverses*. Paris : Maison des sciences de l'homme, 441 p.

Texte législatif

Loi n°001/2018 du 12 janvier 2018 portant révision de la Constitution de la République Gabonaise (J.O. 12 janvier 2018)